

### **REMARKS**

Applicant notes with appreciation the opportunity provided by the Examiner to conduct a telephonic interview. The foregoing amendment amends Claims 2-4, 6, 10, and 18, and adds new Claim 23. Now in the application are Claims 2-23 of which Claims 6, 10, 18 and 23 are independent. No new matter and no new issues are raised by the foregoing amendments. Thus, consideration of the proposed amendments requires no further search. The following comments address all stated grounds for rejection and place the presently pending claims, as identified above, in condition for allowance.

#### **Claim Amendments:**

The amendments to Claims 2-4, 6, 10, and 18 are not meant to address any art rejection. These amendments address informalities in the pending claims to correct issues of dependency caused by the cancellation of claim 1 and to improve readability. New Claim 23 corresponds to original Claim 1 rewritten in a format commensurate with U.S. Patent practice to improve readability of the claimed subject matter.

### **Rejections under 35 U.S.C. §103**

For purposes of clarity in the discussion below, the respective related claim sets will be discussed separately.

#### **A. Rejection of Claim 1 under 35 U.S.C. §103:**

The Office Action rejects Claim 1 as being unpatentable over U.S. Patent No. 5,787,367 of Berra (hereinafter "Berra") in view of U.S. Patent No. 6,401,207 of Funakoshi *et al.* (hereinafter "Funakoshi") and in further view of U.S. Patent No. 5,945,906 of Onuma (hereinafter "Onuma"). Applicants respectfully traverse this rejection on the basis of the following arguments that Berra in view of Funakoshi and in further view of Onuma fails to teach or suggest all elements of Claim 1, as described below, and hence does not obviate the claimed invention.

Applicants have cancelled original Claim 1 and have rewritten the subject matter of original Claim 1 as new Claim 23 to improve the readability thereof. As such, Applicants address the rejection of original Claim 1 as if new Claim 23 stands rejected as being unpatentable over Berra in view of Funakoshi and in further view of Onuma.

Claim 23 is directed to a vehicle controller. The vehicle controller includes a rewritable memory, a controller, and an interface. The rewritable memory is configured to store a security function used to authenticate an external rewriting device to determine whether rewriting to the rewritable memory by the external rewriting device is permitted. The controller is configured to initiate an authentication process to authenticate the external rewriting device using the security function in response to a request to rewrite data held by the rewritable memory. Upon authenticating the external rewriting device the security function stored in the rewritable memory is deleted and a new security function is written into the rewritable memory. The interface is configured to receive and transmit one or more signals between the controller and the external rewriting device.

The rewritable memory is implementable in a non-volatile memory such as, a flash memory, an EPROM, or an EEPROM. Consequently, the invention recited in Claim 23 beneficially allows recovery of a security feature by rewriting security data stored in a rewritable memory and thus *preventing an illegal rewriting* even if the security data has been divulged to a third party.

The Berra reference is directed to a system and method for providing secured programming for reprogramming on-board vehicle computer systems. The on-board vehicle computer system of Berra includes an EEPROM to store a serial identification code, a first password A and a second password B. The serial identification code is used to gain access to a portion of an authorized database, the first password A is a unique numeric code identifying that particular engine control unit and the second password B contains a series of variables that define values used in connection with an encryption function.

To reprogram the Berra on-board vehicle computer system, the disclosed system and method uses an interface tool in communication with the vehicle computer and the authorized database. The interface tool requests the serial identification code from the on-board computer, and in response, the computer transmits the serial identification code to the interface tool, which, in turn, forwards the serial identification code to the authorized database. The authorized database uses the serial identification code to look up and transmit the database copy of the first password A to the vehicle computer via the interface tool.

The password lookup in the authorized database provides the designated first password A, which contains a unique message that is compared with the first password A stored in the vehicle computer. If the first password A from the authorized database matches the first password A stored in the vehicle computer, the database formulates an encryption function as a function of the second password B and a series of data values to produce a series of output values. These output values are transmitted to the vehicle controller via the interface tool where they are deciphered based on the encryption function and second password B to provide a series of deciphered data values. The deciphered data values are compared to the data values stored in the vehicle computer. If the deciphered data values match the stored data values, authorized reprogramming of control software in the engine control unit is allowed.

The Berra reference teaches or suggests an encryption technique for encrypting data written to an on-board computer. The Berra reference does not teach or suggest a controller as recited in Claim 23. That is, the Berra reference does not teach or suggest a controller configured to initiate an authentication process to authenticate an external rewriting device using a security function stored in rewritable memory in response to a request to rewrite data held by the rewritable memory. The controller upon authenticating the external rewriting device causes the security function stored in the rewritable memory to be deleted and causes a new security function to be written into the rewritable memory. It is admitted in the Office Action that the Berra reference does not teach or suggest a vehicle controller configured to write new security data into rewritable memory.

The Funakoshi reference is directed to a vehicle anti-theft system. The anti-theft system of the Funakoshi reference includes a key unit, such as an ignition key and an ECU mounted to the vehicle. The ECU includes a first data generation unit to produce a first data unit. The first data unit is copied by the ECU and provided to the key unit. Both the key unit and the ECU include a key generating unit for generating a key or password needed to decipher encoded data. Accordingly, the key unit (i.e. the ignition key) generates a password from the data unit provided by the ECU and stores the password in memory until needed. In similar fashion, the ECU generates the password from the data unit and stores the password in memory until needed. Accordingly, when

the ignition key is inserted into the ignition or at some time shortly thereafter, the ignition key forwards the password to the ECU and in turn the ECU compares the received password to the password stored in the ECU to authenticate the ignition key to allow operation of the vehicle.

The Funakoshi reference teaches or suggests an encryption technique for use in authenticating an ignition key. Funakoshi solves the problem of an individual making an unauthorized copy of an ignition key at a locksmith or other business and using the unauthorized or unauthentic ignition key to start and drive off in a vehicle without permission from the owner. The Funakoshi reference fails to teach or suggest a controller as recited in Claim 23.

The Onuma reference is directed to a vehicle anti-theft system. The vehicle anti-theft system of Onuma includes a key unit (i.e. ignition key) and an ECU mounted to the vehicle. The key unit includes a memory for storing a transponder I.D. unique to the key unit. The transponder I.D. is used by an immobilizer unit in communication with the ECU to authenticate the transponder I.D. provided by the key unit and take an appropriate security measure should authentication fail. The Onuma reference like the Funakoshi reference solves the problem of an individual making an unauthorized copy of an ignition key at a locksmith or other business and using the unauthorized or unauthentic ignition key to start and drive off in a vehicle without permission from the owner. The Onuma reference does not teach or suggest a controller as recited in Claim 23.

In contrast, Claim 23 recites a controller configured to initiate an authentication process to authenticate an external rewriting device using a security function held in a rewritable memory in response to a request to rewrite data held by the rewritable memory. The controller upon authenticating the external rewriting device causes the security function stored in the rewritable memory to be deleted and causes a new security function to be written into the rewritable memory. That is, the vehicle controller of Claim 23 performs a memory rewrite if a first security function held by the rewritable memory permits and in response to a permissible write receives a new security function from an external rewriting device, deletes the first security function, and writes the new security function into the rewritable memory. The Berra reference does not teach or suggest such a controller. The Examiner recognizes this deficiency in Berra and cites the

Funakoshi reference to bridge the factual deficiencies of Berra. However, the Funakoshi reference teaches a vehicle controller that does not receive a new security function from an external rewriting device. The ECU of Funakoshi receives a password from an ignition key unit, to authenticate the ignition key unit to prevent a taking of the vehicle using an unauthorized ignition key. Moreover, the password received by the ECU of Funakoshi is not a new password. That is, the password provided by the ignition key unit to the ECU is used by the ECU to match a preexisting password to authenticate the ignition key and avoid an unauthorized taking of the vehicle. The Funakoshi reference does not teach or suggest writing of the password received from the ignition key in rewritable memory.

Further, the rolling code function of the Onuma reference is cited as teaching or suggesting the deletion of a first security function in response to receipt of a new security function from an external rewriting device and writing the new security function into the rewritable memory. However, the rolling code feature taught by Onuma takes place completely within the confines of the vehicle and is not received from an external rewriting device.

Neither the Berra reference, nor the Funakoshi reference, nor the Onuma reference, alone or in any combination, teach, suggest, or disclose all the features recited in Claim 23. Only the Berra reference is concerned with rewriting to memory of a vehicle controller. Nevertheless, the Berra reference does not teach or suggest the rewriting of a new security function to a rewritable memory. The Berra reference further fails to teach or suggest the deletion of the first security function in response to the authenticating the external rewriting device. Both the Funakoshi reference and the Onuma reference fail to bridge the factual deficiencies of the Berra reference because they fail to teach or suggest a controller as recited in Claim 23. Moreover, there exists no motivation to combine Berra with either Funakoshi or Onuma. Berra solves a problem caused by reprogramming a vehicle controller without authorization to do so. Both Funakoshi and Onuma solves the problem of an individual making an unauthorized copy of an ignition key at a locksmith or other business and using the unauthorized or unauthentic ignition key to start and drive off in a vehicle without permission from the owner. The Berra reference solves a problem distinct from the problem solved by both

Funakoshi and Onuma. Hence, there exists no common problem to solve amongst the three applied references and therefore there exists no motivation to combine Berra and Funakoshi and Onuma in any combination. *See*, MPEP §2143.01.

Accordingly, neither the Berra reference, nor the Funakoshi reference nor the Onuma reference, alone or in any combination, teach or suggest each and every element of Claim 23. Hence, Applicants respectfully request the Examiner to pass new Claim 23 and dependent Claims 2-5 to allowance.

B. Rejection of Claims 6 and 7 under 35 U.S.C. § 103(a):

The Office Action rejects Claims 6 and 7 as being unpatentable over Berra in view of Funakoshi and in further view of Onuma. Applicants' respectfully traverse this rejection on the basis of the following arguments that Berra in view of Funakoshi and in further view of Onuma fails to teach or suggest all elements of Claims 6 and 7 as described below, and hence, does not obviate the claimed invention.

Claim 7 depends from Claim 6 and thereby incorporates the novel features of Claim 6.

Claim 6 is directed to a rewriting device for rewriting a rewritable memory included in a vehicle controller. The rewriting device includes a memory for storing new security data and a communication means for transferring the new security data to the rewritable memory of the vehicle controller. The transferred new security data written into the rewritable memory and is used to determine whether rewriting to the rewritable memory is permitted.

The Berra reference does not teach or suggest a rewriting device for rewriting a rewritable memory included in a vehicle controller that includes a memory for storing new security data. Neither the Funakoshi reference nor the Onuma reference, alone or in combination, cure the factual deficiencies of the Berra reference. Both the Funakoshi reference and the Onuma reference are not concerned with a rewriting device, rather, each reference is concerned with an ignition key, which is clearly not a rewriting device.

Moreover, there exists no motivation to combine Berra with either Funakoshi or Onuma in any manner. Berra solves a problem caused by reprogramming a vehicle controller without authorization to do so. Both Funakoshi and Onuma solves the problem

of an individual making an unauthorized copy of an ignition key at a locksmith or other business and using the unauthorized or unauthentic ignition key to start and drive off in a vehicle without permission from the owner. The Berra reference solves a problem distinct from the problem solved by both Funakoshi and Onuma. Hence, there exists no common problem to solve amongst the three applied references and therefore there exists no motivation to combine Berra and Funakoshi and Onuma in any combination.

The Berra reference in view of the Funakoshi reference, and in further view of the Onuma reference, fail to teach or suggest each and every element of Claims 6 and 7, and therefore, fail to establish a *prima facie* case of obviousness. Accordingly, Applicants' respectfully request the Examiner to reconsider and withdraw the rejection of Claims 6 and 7 under 35 U.S.C. § 103(a).

C. Rejection of Claim 10 under 35 U.S.C. § 103:

The Office Action rejects Claim 10 as being unpatentable over Berra in view of Funakoshi and in further view of Onuma. Applicants' respectfully traverse this rejection on the basis of the following arguments that Berra in view of Funakoshi and in further view of Onuma fails to teach or suggest all elements of Claim 10, as described below, and hence, does not obviate the claimed invention.

Claim 10 is directed to a memory rewriting system for a vehicle controller. The memory system includes, a vehicle controller, a rewritable memory mounted on the vehicle controller, and a rewriting device for transferring new security data to the vehicle controller. The rewritable memory stores first security data which is used to determine whether rewriting to the rewritable memory is permitted. The vehicle controller is configured to delete the first security data and to write the new security data into the rewritable memory when it is determined that rewriting to the rewritable memory is permitted. The memory rewriting system of Claim 10 enables, even after shipment of a vehicle from the manufacturer, the changing of a key for releasing a security feature that prevents a program or data stored in memory of the vehicle controller from being tampered with. Even if the security feature has been divulged to an unauthorized third party, the vehicle manufacturer can use a rewriting device to change this security feature, thus enabling recovery of the security feature.

The Berra reference teaches or suggests an encryption technique to encrypt data written to an on-board computer. The Berra reference does not teach or suggest a memory rewriting system for a vehicle controller that includes a rewritable memory mounted on the vehicle controller configured to delete first security data and to write new security data into the rewritable memory. Moreover, in the Office Action it is admitted that the Berra reference does not teach or suggest a memory rewriting system for a vehicle controller configured to write new security data into rewritable memory.

The Funakoshi reference teaches or suggests an encryption technique for use in authenticating an ignition key. The Funakoshi reference fails to teach or suggest a memory rewriting system for a vehicle controller having a *rewritable memory* for storing first security data used to determine whether rewriting to the rewritable memory is permitted.

The Onuma reference is directed to a vehicle anti-theft system. The vehicle anti-theft system of Onuma includes a key unit (i.e. ignition key) and an ECU mounted to the vehicle. The key unit includes a memory for storing a transponder I.D. unique to the key unit. The transponder I.D. is used by an immobilizer unit in communication with the ECU to authenticate the transponder I.D. provided by the key unit and take an appropriate security measure should authentication fail. The Onuma reference does not teach or suggest a memory rewriting system for a vehicle controller having a rewritable memory for storing first security data used to determine whether rewriting to the rewritable memory is permitted.

In contrast, Claim 10 recites a memory rewriting system for a vehicle controller having a rewritable memory for storing first security data. The first security data being used to determine whether rewriting to the rewritable memory is permitted. That is, the memory rewriting system of Claim 10 performs a memory rewrite if first security data held by the rewritable memory permits and in response to a permissible write receives new security data from an external rewriting device. The Berra reference does not teach or suggest a memory rewriting system for a vehicle controller having a rewritable memory that writes new security data into rewritable memory. This deficiency in Berra is recognized and the Funakoshi reference is cited to bridge the factual deficiencies of Berra. However, the Funakoshi reference teaches that the described vehicle controller



does not receive new security data from an external rewriting device. The ECU of Funakoshi receives a password from a key unit that is meant to match a password held by the ECU. If the received password does not match the existing password in the ECU it is determined that the ignition key is an unauthorized key. The password provided by the ignition key unit to the ECU should be a matching password to authenticate the ignition key unit, and, hence, is not new security data. Moreover, the Funakoshi reference is not concerned with rewriting to a rewritable memory, but rather, is concerned with enabling or disabling a security function for the vehicle to prevent or allow vehicle operation.

The rolling code function of the Onuma reference is cited as teaching or suggesting the deletion of first security data in response to receipt of new security data from an external rewriting device and writing the new security data into the rewritable memory. However, the rolling code feature taught by Onuma takes place completely within the confines of the vehicle and is not received from an external rewriting device.

Neither the Berra reference, nor the Funakoshi reference, nor the Onuma reference, alone or in any combination, teach, suggest, or disclose all the features recited in Claim 10. Only the Berra reference is concerned with rewriting data to memory of a vehicle controller. Nevertheless, the Berra reference does not teach or suggest the rewriting of new security data the rewritable memory of a vehicle controller. The Berra reference further fails to teach or suggest the deletion of the first security data in response to the receipt of new security data from an external rewriting device. Both the Funakoshi reference and the Onuma reference fail to bridge the factual deficiencies of the Berra reference because they fail to teach or suggest the deletion of first security data and writing new security data into rewritable memory in response to receipt of the new security data from an external rewriting device.

Moreover, there exists no motivation to combine Berra with either Funakoshi or Onuma. Berra solves a problem caused by reprogramming a vehicle controller without authorization to do so. Both Funakoshi and Onuma solves the problem of an individual making an unauthorized copy of an ignition key at a locksmith or other business and using the unauthorized or unauthentic ignition key to start and drive off in a vehicle without permission from the owner. The Berra reference solves a problem distinct from the problem solved by both Funakoshi and Onuma. Hence, there exists no common

problem to solve amongst the three applied references and therefore there exists no motivation to combine Berra and Funakoshi and Onuma in any combination. *See*, MPEP §2143.01.

Accordingly, neither the Berra reference, nor the Funakoshi reference nor the Onuma reference, alone or in any combination, teach or suggest each and every element of Claim 10. Hence, Applicants respectfully request the Examiner to reconsider and withdraw the rejection of Claim 1 under 35 U.S.C. §103.

D. Rejection of Claims 2-5 under 35 U.S.C. § 103(a):

Claims 2-6 are patentable for at least the same reasons set forth above with respect to Claim 23, from which these claims depend. The further recitation of the subject matter in Claims 2-5, provides separate further bases for patentability. Neither the Berra reference, nor the Funakoshi reference, nor the Onuma reference, alone or in any combination teach or suggest the vehicle controller recited in Claim 23.

Accordingly, Applicants' respectfully request the Examiner to reconsider and withdraw the rejection of Claims 2-5 under 35 U.S.C. § 103.

E. Rejection of Claims 7-9 under 35 U.S.C. § 103:

Claims 7-9 are patentable for the same reasons set forth above in connection with Claim 6, from which these claims depend. Claims 7-9 recite further patentable subject matter and each claim provides a separate further basis for patentability. Neither the Berra reference, nor the Funakoshi reference, nor the Onuma reference, alone or in any combination, teach or suggest a rewriting device for rewriting a rewritable memory included in a vehicle controller as recited in Claim 6. Accordingly, Applicants' respectfully request the Examiner to reconsider and withdraw the rejection of Claim 7-9 under 35 U.S.C. § 103.

F. Rejection of Claims 11-17 under 35 U.S.C. § 103:

Claims 11-17 are patentable for at least the same reasons set forth above with respect to Claim 10, from which these claims depend. The further recitation of patentable subject matter in Claims 11-17, provides separate further bases for patentability. Neither

the Berra reference, nor the Funakoshi reference, nor the Onuma reference, alone or in any combination, teach or suggest a memory rewriting system for a vehicle controller as recited in Claim 10. Accordingly, Applicants' respectfully request the Examiner to reconsider and withdraw the rejection of Claims 11-17 under 35 U.S.C. § 103.

G. Rejection of Claims 18-22 under 35 U.S.C. § 103:

The Office Action rejects Claims 18-22 as being unpatentable over Berra in view of Funakoshi and in further view of Onuma. Applicants' respectfully traverse this rejection of the basis of the following arguments that Berra in view of Funakoshi and in further view of Onuma fails to teach or suggest all elements of Claim 18, as described below, and hence does not obviate the claimed invention.

Amended Claim 18 is directed to a method for rewriting data stored in a rewritable memory in a vehicle controller. The claimed method includes a step of receiving new security data transferred from an external rewriting device to the vehicle controller and deleting first security data stored in the rewritable memory. The first security data is used to determine whether rewriting to the rewritable memory is permitted. The method writes the new security data into the rewritable memory if permitted.

Claims 19-22 depend directly or indirectly, from amended Claim 18 and thereby incorporate the patentable features of amended Claim 18.

The Berra reference teaches or suggests an encryption technique to prevent unauthorized rewriting of an on-board computer. The Berra reference does not teach or suggest a memory rewriting system for a vehicle controller that includes a rewritable memory mounted on the vehicle controller configured to delete first security data and to write new security data into the rewritable memory. Moreover, it is admitted in the Office Action that the Berra reference does not teach or suggest a memory rewriting system for a vehicle controller configured to write new security data into rewritable memory.

The Funakoshi reference teaches or suggests an encryption technique for use in authenticating an ignition key. The Funakoshi reference fails to teach or suggest a

method for rewriting data stored in a rewritable memory in a vehicle controller as recited in amended Claim 18.

The Onuma reference is directed to a vehicle anti-theft system. The vehicle anti-theft system of Onuma includes a key unit (i.e. ignition key) and an ECU mounted to the vehicle. The key unit includes a memory for storing a transponder I.D. unique to the key unit. The transponder I.D. is used by an immobilizer unit in communication with the ECU to authenticate the transponder I.D. provided by the key unit and take an appropriate security measure should authentication fail. The Onuma reference does not teach or suggest a method for rewriting data stored in a rewritable memory in a vehicle controller as recited in amended Claim 18.

In contrast, amended Claim 18 recites a method for rewriting data stored in a rewritable memory in a vehicle controller that includes a step of deleting first security data stored in the rewritable memory if it is determined rewriting to the rewritable memory is permitted. The first security being used to determine whether rewriting to the rewritable memory is permitted. That is, the method of amended Claim 18 performs a memory rewrite if first security data held by the rewritable memory permits. The Berra reference does not teach or suggest a step of writing new security data into the rewritable memory as recited in amended Claim 18. The Examiner recognizes this deficiency in Berra and cites the Funakoshi reference to bridge the factual deficiencies of Berra. However, the Funakoshi reference teaches that the described vehicle controller does not receive new security data from an external rewriting device. The ECU of Funakoshi receives a like password from a key unit, to authenticate the key unit, however, the received password is not new, and Funakoshi does not delete first security data stored in the rewritable memory if the passwords match. The password provided by the key unit to the ECU should be a matching password to authenticate the key unit, and, hence, is not new security data. Moreover, the Funakoshi reference is not concerned with rewriting to a rewritable memory, but rather, is concerned with enabling or disabling a security function for the vehicle to prevent or allow vehicle operation.

The rolling code function of the Onuma reference is cited as teaching or suggesting the deletion of first security data in response to receipt of new security data from an external rewriting device and writing the new security data into the rewritable

memory. However, the rolling code feature taught by Onuma takes place completely within the confines of the vehicle and is not received from an external rewriting device.

Neither the Berra reference, nor the Funakoshi reference, nor the Onuma reference, alone or in any combination, teach, suggest or disclose all the features recited in amended Claim 18. Only the Berra reference is concerned with rewriting to memory of a vehicle controller. Nevertheless, the Berra reference does not teach or suggest the writing of new security data the rewritable memory of a vehicle controller. The Berra reference further fails to teach or suggest the deletion of the first security data in response to the receipt of new security data from an external rewriting device. Both the Funakoshi reference and the Onuma reference fail to bridge the factual deficiencies of the Berra reference because they fail to teach or suggest the deletion of first security data and writing new security data into rewritable memory in response to receipt of the new security data from an external rewriting device.

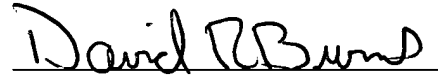
Moreover, there exists no motivation to combine Berra with either Funakoshi or Onuma. Berra solves a problem caused by reprogramming a vehicle controller without authorization to do so. Both Funakoshi and Onuma solves the problem of an individual making an unauthorized copy of an ignition key at a locksmith or other business and using the unauthorized or unauthentic ignition key to start and drive off in a vehicle without permission from the owner. The Berra reference solves a problem distinct from the problem solved by both Funakoshi and Onuma. Hence, there exists no common problem to solve amongst the three applied references and therefore there exists no motivation to combine Berra and Funakoshi and Onuma in any combination. *See*, MPEP §2143.01.

Accordingly, neither the Berra reference, nor the Funakoshi reference nor the Onuma reference, alone or in any combination, teach or suggest each and every step of Claims 18-22, as amended. Hence, Applicants respectfully request the Examiner to reconsider and withdraw the rejection of Claims 18-22 under 35 U.S.C. §103.

**CONCLUSION**

For the foregoing reasons, Applicants contend that Claims 2-23 define over the cited art. If there are any remaining issues, an opportunity for an interview is requested prior to the issuance of another Office Action. If the above amendments are not deemed to place this case in condition for allowance, the Examiner is urged to call Applicants' representative at the telephone number listed below.

Respectfully submitted,  
LAHIVE & COCKFIELD, LLP



David R. Burns  
Reg. No. 46,590  
Attorney for Applicants  
28 State Street  
Boston, MA 02109  
(617) 227-7400  
(617) 742-4214

Date: August 5, 2004